DET IT Security Standards by NIST Family

NIST 800 53 r4 CONTROL FAMILY	NIST ID	DESCRIPTION/PURPOSE
Audit and Accountability	AU	The standards listed in this section focus on: (i) create, protect, and retain IT system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate IT system activity; and (ii) ensure that the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.
Appropriate Use of Software Standard		The standards listed in this section focus on how to utilize (purchase, use, install, and/or access) software for IT systems and system environments. CM-10, CM-11, MP-4, MP-5, MP-6, MA-5, SA-2, SI-7
Security Assessment and Authorization	CA	The standards listed in this section focus on requirements to: (i) periodically assess the security controls in IT systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in IT systems; (iii) authorize the operation of IT systems and any associated IT system connections; and (iv) monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management	CM	The standards listed in this section focus on how to: (i) establish and maintain baseline configurations and inventories of IT systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for IT technology products employed in IT systems.
Contingency Planning	CP	The standards listed in this section focus on how to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for IT systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Data Classification Standard		The standards listed in this section focus on information assets being identified, categorized, and labeled as Classified, Restricted, Sensitive, or Public to facilitate the use of appropriate security, privacy, and compliance measures to protect the confidentiality, integrity, and availability of data/information. AC-21, AC-22
Encryption Standard		The standards listed in this section focus on: (i) the use of encryption and cryptographic services/tools; and, (2) when/where encryption is required for data and IT systems/environments. AC-19, SC-8, SC-12, SC-13, SC-28

Identification and Authentication	IA	The standards listed in this section focus on how to identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to IT systems.
Incident Response	IR	The standards listed in this section focus on how to: (i) establish an operational incident-handling capability for IT systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate officials and/or authorities.
Maintenance	MA	The standards listed in this section focus on how to: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection	MP	The standards listed in this section focus on how to: (i) protect IT system media, both paper and digital; (ii) limit access to information on IT system media to authorized users; and (iii) sanitize or destroy IT system media before disposal or release for reuse.
Mobile Device Standard		The standards listed in this section focus on the security requirements for the use of laptop computers and mobile devices (e.g. tablet, cell phone, PDA, smart watch, etc.) to access confidential or restricted data. AC-3, AC-7, AC-19, MP-6, SC-13, SC-28.
Password Standard		The standards listed in this section focus on the minimum requirements for password use by account type. IA-5, AC-7, AC-20, AU-2.
Patch Management Standard		The standards listed in this section focus on the requirements to develop, document, maintain, and execute IT system patch schedules and plans to meet compliance regulations and security best practices. SI-2
Physical and Environmental Protection	PE	The standards listed in this section focus on how to: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Security Planning	PL	The standards listed in this section focus on how to develop, document, periodically update, and implement security plans for IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.
Personnel Security	PS	The standards listed in this section focus on how to: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that

		organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Remote Access Standard		The standards listed in this section focus on: (i) documenting business need for remote access to IT systems and information; restrictions for remote access to IT systems and information; security requirements for IT systems and information that may be accessed remotely. AC-2, AC-3, AC-17, AC-20, SC-10
Risk Assessment	RA	The standards listed in this section focus on how to periodically assess the risk to operations (including mission, functions, image, or reputation), assets, and individuals, resulting from the operation of IT systems and the associated processing, storage, or transmission of information.
System and Services Acquisition	SA	The standards listed in this section focus on how to: (i) allocate sufficient resources to adequately protect IT systems; (ii) employ system development life cycle processes that incorporate IS considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection	SC	The standards listed in this section focus on how to: (i) monitor, control, and protect communications (i.e., information transmitted or received by IT systems) at the external boundaries and key internal boundaries of the IT systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective IS within IT systems.
System and Information Integrity	SI	The standards listed in this section focus on how to: (i) identify, report, and correct information and IT system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within IT systems; and (iii) monitor IT system security alerts and advisories, and take appropriate actions in response.
Vulnerability Management Standard		The standards listed in this section focus on: (i) vulnerability assessment scans of IT systems and environments; and, (ii) documentation and remediation or acceptance of vulnerabilities. R1-1, RA-5
Wireless Access Standard		The standards listed in this section focus on technical controls to secure wireless local area networks and wireless access. AC-3, AC-18, IA-6, PE-3, PE-19, SC-8, SC-13, SC-15
Program Management	PM	The standards listed in this section complement the security controls in the security control families by focusing on the organization-wide information

		security requirements that are essential for managing information security programs.

Source: Adopted from DOA/DET IT Security Standards, MARS-E 2 Minimum Acceptable Risk Security and Privacy Controls for Exchanges, and NIST 800-53 r.4

Author: T. Choice, 11/21/17